



UNCLASSIFIED



COUNTER IMPROVISED EXPLOSIVE DEVICES CENTRE OF EXCELLENCE

CTRA M-618 KM 10,400. 28240 HOYO DE MANZANARES - MADRID. SPAIN

PtF 2013/142

To see distribution list

Date: 05 March 2013

Subject: Final report 2nd C-IED COE Lessons Learned Workshop, 03-05 Dec 2012.

1. Introduction

The Counter Improvised Explosive Devices Centre of Excellence (C-IED COE) conducted its second C-IED COE Lessons Learned workshop 03-05 December 2012 at the C-IED COE, Hoyo de Manzanares in Spain. The workshop was open for NATO Commands, Partnership for Peace, ISAF Contributing Nations and EDA.

The overarching topic of the workshop was:

“How Lessons Learned can add value to C-IED operations and equipment”.

2. Aim

The aim of the workshop was to achieve the following objectives:

- To conduct open discussions on the presented subjects;
- To develop links with the C-IED COE and its capabilities;
- To provide an opportunity to share information and to network with the C-IED Community of Interest (CoI).

3. Main topics

Based on identified challenges and operational deficiencies in the field of C-IED the C-IED COE had chosen the following topics for the workshop:

- Technology in support of C-IED.
- TTPs update from theatre and on pre-deployment training.
- Ways to improve Level 1 exploitation.

UNCLASSIFIED

4. Structure

Introduced by three briefings, each topic of the above listed was discussed for one day. These briefings were provided by different nations or agencies. They gave a different perspective on the subject. The briefings followed a short Question and Answer (Q&A) period. Afterwards the audience / attendees were divided in three syndicates. Each syndicate discussed a sub-theme of the main topic. The syndicates were requested to provide a short presentation during the plenary discussion on the findings and possible solutions.

5. Overall findings

During the workshop several lessons were identified. They can be found together with a discussion on the rationale, with recommendations and current statuses at Annex B.

Regardless the fact, that the three different main themes listed above were discussed, some subjects dominated the findings of all syndicates: Institutionalisation of C-IED and again one finding of last year's Lessons Learned workshop: C-IED information management.

5.1. Institutionalisation of C-IED

C-IED needs to be institutionalized at all levels in the nations. This includes the implementation of a C-IED Lessons Learned process. However, there was a common understanding, that there is no common standard how to "institutionalise" C-IED. Institutionalisation can be seen as a common functionality of all measure including development and procurement of new technology, operational use of the technology, training and education as well as an appropriate consideration of C-IED expertise at all staff levels. The aim must be, to have a complete package allowing the operational units to be trained and equipped as they fight. This includes appropriate consideration of C-IED in NATO exercises as well as development of e-learning and deployment of mobile training teams. Institutionalisation can be seen as a moderator to finally implement C-IED in peacetime and in operations. It must be implemented on all command levels.

5.3. C-IED Information Management

Again, similar to the result of last year's C-IED Lessons Learned workshop the general lack of communications and information exchange as well as the existing overflow of sources with C-IED information was highlighted. The risk of a "black hole" related to operational C-IED information going along with the transition of responsibilities in ISAF beyond 2014 cannot be excluded. The ambitious process of the C-IED COE to take a mediator role through the development of a C-IED information exchange process supported by the establishment of unclassified and classified C-IED informational portals has been initiated, but the establishment of a common agreed information handling and exchange process supported by

UNCLASSIFIED

information portals is complex. Still a major concern is the over-classification of information and the limited willingness of nations and agencies to share information.

5.4. Way ahead

The C-IED COE has taken over the responsibility for the content management for the C-IED BICES informational portal and will take over the content responsibility for the ACT C-IED informational portal in the first half of 2013. This will allow a content review of both portals out of one hand. Both portals will have a Lessons Learned portion and to a certain extent an operational historical data base. Furthermore the COE is developing a data base on C-IED equipment and technology as a single source option. This data base will be unclassified and posted on the portals.

The information exchange between the COE and nations and JIEDDO is increasing. This provides valuable information for all COE products and the courses provided by the COE. Therefore all users of the portals and all course attendants are having a benefit of this improving process.

All these measures will improve the information exchange amongst the C-IED community of interest and will support the institutionalisation of C-IED.

6. Further workshops

The workshop was considered to be of great value for the community of interest. The next Lessons Learned workshops will be in 3 -5 December 2013.

FOR THE COUNTER IMPROVISED EXPLOSIVE DEVICES CENTRE OF EXCELLENCE



Santiago San Antonio Demetrio
Colonel, ESP Army
C-IED COE Director

List of annexes

- A. Workshop topics
- B. Workshop observation/Lessons Identified
- C. List of participants

Distribution list:

Action:

ACT Distribution List III
ACT Distribution list V
ACT Distribution List VI

ACT IPT
ACT LL
JALLC
HQ ISAF C-IED Branch
ISAF HQ IJC C-IED Branch
SHAPE OPI OPS
JFCB DCOS OPS
JC LB DCOS OPS
HQ FC Madrid
HQ FC Heidelberg
NRDC Turkey
NRDC Spain
NRDC Italy

NSHQ
JWC
JFTC
NATO School
NATO JEWCS

COE DAT
COE EOD
COE C2
COE MILENG
JIEDDO
CFC
COS EUROCORPS
EDA
COS GE-NL CORPS

Information:

C-IED COE Sponsoring Nations
LL WS Participants

ANNEX A – Workshop topics and briefers

Topic 1: Technology in support of C-IED.

Since the start of the ISAF operations, technology has improved the effectiveness and efficiency of C-IED operations. Military search, Route Clearance, WIT equipment, IEDD equipment, ISR/air assets, ESM/ECM, vehicle and personnel safety equipment use technology in support of C-IED. What are the latest national developments of the technology in use? These technologies seem to have no limits. But latest observations in theatre indicate insufficiency. What kind of technology is useful for troops? Which not? What are the limitations of detection capabilities? How effective are blast effect mitigation techniques in use? Technology is not the answer for problems, it is a tool soldiers at tactical and on command level are using to finally reduce the C-IED threats and effects. What are strengths and limitations? To which extent simulation can be used in C-IED training?

Subtopics:

- 1.1. Technology for force protection: active or passive assets
- 1.2. Technology available for training and their limitation
- 1.3. Strengths and limitations for technology

Briefers:

Briefer	Topic
Lt Col James GARVEN	"Procurement and the introduction new technologies" (GBR/LWDG)
Cdr Leonard HAIDL	"Technology in support of C-IED" (USA / JIEDDO)
Col Rafael JIMENEZ	"Detection : nano technology" (SPAIN)

Topic 2: TTPs update from theatre and on pre-deployment training.

Adversaries in theatres are adapting frequently their TTPs. New equipment and technology requires a TTP/training update and/or a new development of own TTPs. Are all soldiers trained to use this technology at any time? What are latest acknowledged changes to adversaries TTPs? How do they have influenced own pre-deployment training? How fast can we change TTPs? Do we want exchange TTP information with host nation and non-military actors?

Subtopics:

2.1. Pre-deployment training with update on TTPs

2.2. What factors define insurgents TTPs and how will those be identified and disseminated as the force transitions responsibility to ANSF?

2.3. Support to host nation and non-military actors: LI/LL from transition of responsibility to ANSF/non military actor

Briefers:

briefer	Topic
Lt Col James GARVEN	"TTPs and their evolution" (GBR / LWDG)
Mr Mark BENN	"ATO assets and TTPs for training" (USA / JIEDDO JET)
Col Rafael JIMENEZ	"Problem base approach and lessons Identified" (SPAIN/IDC)

Topic 3: Ways to improve Level 1 exploitation:

Exploitation is a cross functional C-IED activity that affects all three pillars of C-IED: Attack the Network, Defeat the Device and Prepare the Force. The first level of exploitation – Level 1 – is as important as the other two levels, however not all nations are conducting the evidence collection and the initial forensic process in a standardised way.

How could we support and improve the tactical level exploitation (Level-1)? Are the WIT teams correctly configured? Are the Level 1 reports produced following a standard format? Covers the format used in ISAF the requirements? How could Level 1 benefit from current technologies and improve quality of the reports? What aspects from an operational, judicial and intelligence perspectives are missing in these reports? Are there any obstacles between Level-1 and Level-2? Does the tactical level receives the required feed back in time to support own operations in their AOR? What works and what does not work? Do we need to develop an exploitation lexicon?

Subtopics:

- 3.1. How we can improve level 1 exploitation?
- 3.2. Do we need different reporting systems to support both intelligence operations and transition to host nation rule of law?

Briefers:

briefer	Topic
Maj Gabriel PLUS	“MNTel 2 procedures” (FRA / ENGINEER SCHOOL)
Mr Thomas O’BRIEN	“Exploitation level1” (JIEDDO / brief from TF PALADIN side)

ANNEX B – Observation/Lessons Identified during the workshop.

1. Observation/Lessons Identified.

Some of the technology in use is not user-friendly and requires extensive training. Some of the equipment is not reaching the expected operational effectiveness. During the R&D phase the testing processes for technology are providing results different to those the equipment shows during operations.

Discussion

There needs to be a strong relation between technology, TTPs and personnel training. Interaction between industry and military is required to achieve user-friendliness to the biggest extent possible. E.g. UK is inviting industry for their Mission Exploitation Symposiums to allow direct interaction between industry and operational units in addition to the established LL-process. A continued investment in the development of technology is needed.

Recommendations:

- a. Nations should verify the effectiveness of their processes between military and industry to **improve the user-friendliness of technology**.
- b. Based on a **Lessons learned process**, there is a need for the development of a **fast info exchange process** between military and industry to influence R&D processes.

2. Observation/Lessons Identified.

There is a trend to an increasing confidence in the use of technology alone in operations.

Discussion

It is important to understand and apprehend that technology is a tool and not always the solution. The use of technology like e.g. Route Clearance Packages, Ground Penetration Radars, ISR assets are not useful to its full extent in all operational environments. Training of tactical level units on basic skills like Ground Sign Awareness must be continued on a high standard to meet the general principle "train as you fight".

Recommendation:

Training of tactical units in manual skills needs to be conducted and adapted to the operational environment on a high standard as it will help to maintain the **right balance between use of technology and soldiers education**.

3. Observation/Lessons Identified.

The use of advanced technology and simulation can support training.

Discussion

Modern technology can be used to provide realistic operational scenarios for all operational levels. Simulation can provide effective and cheap training options to train personnel effectively and quick without the need to deploy the units to exercise areas. This is especially of utmost importance in times of tight financial limitations. However, there is a need for a balanced assessment between the principle to “train as you fight” in a realistic operational environment and the use of technology and simulation for certain training phases.

Recommendations:

- a. NATO and nations are enhancing the use of simulation technology in the training process.
- b. **As part of an institutionalization process for C-IED on each level**, develop C-IED simulation technology and implement in the training loop.

4. Observation/Lessons Identified.

The technology in use is sometime complicated and soldiers are not aware on the capabilities of the equipment.

Discussion

The technology in use provides a higher survivability on the battlefield. It is important that the users understand the technologies capabilities and limitations. Observations concerning difficulties of operators using technology and equipment need to be reflected in the Lessons Learned reporting to be considered in the training.

Recommendation

Improve training to **increase awareness** about capabilities and limitations of technology/equipment.

5. Observation/Lessons Identified.

Changing TTPs in theatre need to be considered as soon as possible in pre-deployment training. Sometimes the time from an observation until the consideration in pre-deployment training is too slow.

Discussion

There are different approaches to generate Lessons Learned from theatre, but not all accommodate the need of a quick feed back to influence national pre-deployment training.

Some nations have embedded LL personnel in theatre, others are using a feedback process after being redeployed, e.g. joint seminars or workshop. Latest can cause a

time delay to implement required amendments to the pre-deployment training. Very often the training organisation is too slow to react and to adapt to new observed threats, too. A quick adaptation of pre-deployment training based on recent observed changes to TTPs is key to safe lives.

Recommendations

- a. **Dedicated LI/LL specialist should be deployed and embedded in theatre** at all operational levels.
- b. **Instructors of pre-deployment training facilities** should be deployed to theatre to provide immediate feedback to adapt the training already during their deployment and/or immediately after their return.
- c. A regular and **quick reporting system** needs to be established.

6. Observation/Lessons Identified.

Some HQs and Staffs are not having dedicated C-IED expertise and/or not considering C-IED aspects.

Discussion

Senior leaders/commanding officers are often underestimating the requirement to establish an effective C-IED orientated staff organisation. National caveats, limited training expertise and different operational views hamper both appropriate considered staff organisation and RIP-training. The mindset for the Attack the Network concept is not fully understood. Main emphasis still lays on Defeat the Device and Prepare the Force.

Recommendations

- a. Conduct **Senior Leadership C-IED training**.
- b. As part of **institutionalisation of C-IED** revise job descriptions of NATO Command Structure and NATO Force Structure HQs to consider C-IED expertise.
- c. **Revise staff organizations** to consider a C-IED staff functionality.
- d. C-IED needs to be an **exercise training objective** for NATO exercises.

7. Observation/Lessons Identified.

With the transition of operational responsibilities to ANSF C-IED reporting will decrease in quantity and quality.

Discussion

Cultural behavior, minimal understanding of C-IED processes in ANSF and lack of appropriate training, equipment and special trained personnel will reduce the quantity and quality of IED reports.

Recommendations

- a. **Emphasize the key role of C-IED reporting** during the ANSF transition.
- b. **Train ANSF in CIED-Reporting**.

8. Observation/Lessons Identified.

Based on Lessons Identified from operations in Iraq a risk of a “black hole” of intelligence as a result of the draw down of ISAF troops cannot be excluded.

Discussion

It cannot be excluded that the transition of responsibilities towards ANSF will go along with reduced intelligence gathering, reduced exploitation of IED events and finally with reduced knowledge of network and insurgent activities. Level 1 exploitation will be hampered by cultural behavior; a limited number of trained specialist and lack of appropriate and well maintained equipment as well as the currently not foreseeable success the development of an effective AFG Level 2 exploitation capability will support this trend. This is supported by the current coalition force dissemination practices to exclude ANSF from the benefits of a detailed and effective C-IED reporting system.

Recommendations

- a. Establish a “**2 way street**” between CF and ANSF through military and/or law enforcement cooperation to develop a high level of exploitation (beyond AFG national capabilities) and maintain a information exchange on highest standard possible.
- b. **Emphasize the importance of evidence collection and exploitation** for an effective Attack the Network process during the ANSF transition.
- c. **Identify ANSF exploitation capability gaps.**
- d. Support the establishment of appropriate **exploitation structures and capabilities.**

9. Observation/Lessons Identified.

Some nations still not have developed a sufficient Weapons Intelligence Team training.

Discussion

Personnel need to be trained before deployment into theatre. But some nations still have a limited capability to train WIT level 1 teams. Training provided by other nations and NATO is cost extensive due to the length of training.

Recommendations

- a. **Develop a long distance learning system** with e-learning to reduce length of WIT courses.
- b. **Develop WIT “train the trainer” courses** for futures teachers.
- c. Offer WIT **mobile training teams** to support national training.

10. Observation/Lessons Identified.

Exploitation results are often not disseminated to tactical level units.

Discussion

Tactical level units often complain that they are not included in the dissemination chain for exploitation results and they receive those results too late. One reason for that is the backlog of IED cases in the Level 2 laboratories. Another reason is a misunderstanding of the information dissemination process and its structure.

Level 2 laboratories cannot disseminate all reports to any tactical unit. However, level 2 laboratories provide periodic updates (tactical and technical) to level 1 teams about trends and provide guidance concerning observed weaknesses of search or collect evidences in their Area of Operation (AoR). In addition, level 2 laboratories in coordination with the Theater Explosive eXploitation cell (TEX) and J2 provide periodic updates to J3 about tactical and technical situation for their AoR and neighboring areas. For example, MNTEL 2 provide a fortnightly brainstorming about Kabul area coordinated with level 1 and ISAF C-IED branch. The TEX cell has been created to collect and manage all level 2 reports from the AoR and to include them into the CIDNE and other data bases. This is a push-pull system. Through CIDNE data base, the tactical level with the J2 and/or J3 can pull this information to support their operations and counter IED network activities. The information flow exists between the stakeholders.

Recommendations

- a. Improve understanding **about WIT report classification** and dissemination system during WIT training and WIT courses.
- b. ISAF IJC C-IED reviews the SOP 10371 "IED Exploitation", dated 02 Jan 2012 to reflect the ISAF exploitation feedback process.

11. Observation/Lessons Identified.

The ISAF WIT exploitation process report is not adapted to Afghan requirements and the national prosecution process.

Discussion

There is a need for a different reporting system to support both the Afghan national intelligence operations and the transition from ISAF to the host nation rule of law.

The ISAF reporting system is using a specific software which requires specific computer skills to feed the CIDNE data base. In contrary, the current ANSF WIT report system is based on written report not using photos and or a computer network.

The reporting system must reflect host nation capabilities and constraints. The WIT Level 1 reporting are the essential inputs to the prosecution process. IED activity is a criminal act requiring prosecution under host nation laws. Evidences are only

UNCLASSIFIED

admissible if collected by/with AFG. Empowering Afghan solution selected with ISAF support is the best way.

Recommendation

Support the development of an **AFG reporting system adapted to the AFG requirements.**

12. Observation/Lessons Identified

C-IED information are over-classified and the willingness to share information and evidences between nations is not supporting effective counter network activities.

Discussion

There is constant discussion ongoing that C-IED information are over-classified and nations are not willing to disseminate information to full extent. In November 2012, JALLC has released a study addressing the questions concerning the classification and releasability of information and provides recommendations, how to address the subject. In this report, JALLC recommends SHAPE and HQ SACT endeavour to support and maintain the Bi-SC Handbook on Information and Intelligence Sharing (I&IS) with Non NATO Entities (NNE) as a tool to foster understanding of the NATO Security Policy for HQ and working environment. The one line version of I&IS portal should be replicated to mission and Unclassified networks to the extent classification permits for dissemination. This way should provide awareness of Policy changes to security personnel and better understanding classification markings in NATO. According to JALLC, all NATO personnel should ensure that documents written are appropriately classified and, where necessary, paragraph marked with downgrade instructions. Senior Leaders must ensure that markings recommendations are applied for all documents of Nato Confidential or higher that they sign. In last, SHAPE should amend the Comprehensive Operations Planning Directive to provide some examples or templates illustrating best practices in this subject to establish right information exchange requirements. The NATO Crisis Response System Manual (NCRSM) should be amended with the last needs and successes of Operation UNIFIED PROTECTOR to facilitate information sharing.

Recommendation

NATO organisations and nations are **paying attention to the recommendations of the JALLC report.**

UNCLASSIFIED

ANNEX C – List of participants

A total of 58 persons attended the C-IED COE workshop.

Country	Attendees no	Country	Attendees no
Austria	1	Italy	3
Belgium	3	Netherlands	2
Hungary	2	Norway	4
Canada	4	Slovakia	1
Denmark	1	Slovenia	2
Finland	2	Spain	10
France	4	Sweden	3
Germany	5	United States	7
Great Britain	4		

Organization (not all are listed)	Country
EDA	
SHAPE	
NATO - ACT	
NATO - ACO	
NATO - HQ NATO Rapid Deployment Corps - Turkey	
NATO - HQ NATO Joint Force Command - Naples	
NATO - HQ NATO Joint Force Command - Brunssum	
HQ Eurocorps	
Engineer School	Austria
Operations & Training - Doctrine and Requirements Division	Belgium
CIED Task Force / Lessons learned branch	Canada
Joint Service C-IED Branch, Army Operational Command	Denmark

UNCLASSIFIED

UNCLASSIFIED

Defense and Army Command Finland Operations Division	Finland
Joint Explosive Ordnance Warfare Centre	France
<ul style="list-style-type: none"> • German MOD, JOINT OPERATION STAFF • Army Office / CIED Division 	Germany
<ul style="list-style-type: none"> • Lessons Exploitation Centre / LWDG • EOD Regiment 	Great Britain
<ul style="list-style-type: none"> • NCO Academy / CIED team 	Hungary
<ul style="list-style-type: none"> • Italian Counter IED centre • Italian Joint HQ / LL Division • Italian Joint Operation Headquarters 	Italy
JTF C-IED	Netherlands
<ul style="list-style-type: none"> • NOR Army Land Warfare Centre • JWC • NOR military police unit 	Norway
General Staff of the Slovak Army	Slovakia
Combat Training Centre	Slovenia
<ul style="list-style-type: none"> • Intelligence and EOD exploitation Joint Army Forces • Spanish Land Forces HQ • Engineer school / EOD centre 	Spain
Weapon intelligence 133SKV/LG	Sweden
<ul style="list-style-type: none"> • JIEDDO (JMRC, JCOE, JET, J5) • FBI/TEDAC 	United States

UNCLASSIFIED

FIRST NAME	SURNAME	NATIONALITY	RANK	ORGANISATION/UNIT	email
Bruno	DENIS	BEL	OF-3	CC LAND DTM	bruno.denis2@mil.be
Igor	DUIJSTERS	BEL	OF-1	CC LAND DTM	Alain.gysels@mil.be
Arne	VAN LOO	BEL	OF-3	ACOS Ops & Trg	arne.vanloo@mil.be
Keith	MOODY	CAN	OF-4	JFC Naples/OPS/J3/5/OSS	k.moody@jfcnp.nato.int
David	GOULET-DIONNE	CAN	OR5	CFSME	-
Sebastien	NILES	CAN	OF-3	C-IED TASK FORCE	SEBASTIEN.NILES@forces.gc.ca
Derek	SPENCER	CAN	OF-3	NATO Rapid Deployable Corps – Turkey	DEREK.SPENCER@forces.gc.ca
Jörg	BORCHERT	DEU	OF-4	Federal MoD, Strategy and Operations Directorate	JoergBorchert@bmvg.bund.de
Klaus	HARRER	DEU	OF-4	ARMY OFFICE / CIED DIVISION	KlausHarrer@bundeswehr.org
Uwe	HÖLLGER	DEU	OF-4	German Bundeswehr	uwehoellger@bundeswehr.org
Thomas	UHL	DEU	OF-3	MOD	thomasuhl@bundeswehr.org
Michael	WALZ	DEU	OF-4	HQ SACT, C-IED IPT	michael.walz@act.nato.int
Manuel	GOMEZ REYES	ESP	OF-3	NATO JOINT FORCE COMMAND HQ BRUNSSUM	Manuel.Gomez@jfcbs.nato.int
Felipe	JIMENEZ LOPEZ	ESP	OF1	BZAP XV	fjmi108@et.mde.es
Rafael	JIMENEZ SANCHEZ	ESP	OF5	international demining Center	-
Juan	PEREZ RODRIGUEZ	ESP	OF-3	MANDO DE INGENIEROS	Jperr36@oc.mde.es
Juan Ignacio	GOMEZ MONTAÑEZ	ESP	OR-7	HQ Eurocorps	monthly77@hotmail.com
Ramón Javier	PACHECO MORENO	ESP	OR-7	HQ Eurocorps	jav_tomcat@hotmail.com
Sergio	VALBUENA	ESP	OF-2	HQ EUROCORPS	svalgo1@et.mde.es
Jesus Manuel	MARTINEZ VICTORIA	ESP	OF-3	II BANDERA PARACAIDISTA - BRIPAC	Jmarvi1@et.mde.es
Jose Luis	GALVEZ BARRAYA	ESP	OF-2	INTEL CENTER OF THE ARMED FORCES	igalbar@et.mde.es
Santiago	GARCIA RAMOS	ESP	OF-1	CLAEX/CEOD	sgarram@ea.mde.es
Vesa	LAITONEN	FIN	OF-4	DEFENSE COMMAND/ OPS DIV J3	vesa.laitonen@mil.fi
Pekka	ROMPPANEN	FIN	OF-3	ARMY COMMAND	pekka.romppanen@mil.fi
Philippe	MARQUEZ	FRA	OF-4	Joint Explosive Ordnance Warfare Centre	philippe.marquez@intradef.gouv.fr
Gabriel	PLUS	FRA	OF-3	MILITARY ENGINEER SCHOOL	gabriel.plus@intradef.gouv.fr
Ronan	QUINIYOU	FRA	OF-3	Joint Explosive Ordnance Warfare Centre	ronan.quiniyou@intradef.gouv.fr
Pierre	TENAILLEAU	FRA	OF-4	FCHD / DJSE2 / FE / JCC / OPSS	pierre.tenailleau@fchd.nato.int
Jim	BLACKBURN	GBR	CIV	EDA	jim.blackburn@eda.europa.eu

Keith	EMMERSON	GBR	OF-4	SHAPE / SO CIED	Keith.EMMERSON@shape.nato.int
James	GARVEN	GBR	OF-4	LWDG	james.garven544@mod.uk
Stephen	SHORTIS	GBR	OF-2	11 EOD Regt, Royal Logistic Corps	Stephen.Shortis128@mod.uk
Sandor	BABOS	HUN	OF1	NCO ACADEMY CIED TEAM	sandor.babos@mil.hu
Zoltan	BALAZS	HUN	OR7	NCO ACADEMY CIED TEAM	balaszoltan80@gmail.com
Andrea	ANZUINI	ITA	OF2	ITALIAN AIR FORCE / CeO C-IED	andrea.anzuini@aeronautica.difesa.it
Massimo	CROCCO BARISANO	ITA	OF-4	ITALIAN JOINT OPS HQ /LL DIVISION	AVAC.SECTION3@COL.DIFESA.IT
Fabio	SANDONNINI PUNZI	ITA	OF-4	ITA Joint Operational HeadQuarters	j3@coi.difesa.it
Chris	VAN DER LUGT	NLD	OR9	JTF CIED	ctm.vd.lugt@mindex.nl
Marcel	VAN KAAM	NLD	OF-2	JTF CIED	Mpi.v.kaam.01@mindex.nl
Erik	FUNDINGSRUD	NOR	OF-3	NOR ARMY LAND WARFARE CENTRE	efundingsrud@mil.no
Morten	HOGSETH	NOR	OF-2	NORWEGIAN MILITARY POLICE UNIT	MOHOGSETH@MIL.NO
Bjoern-Tore	SKREDLUND	NOR	OF-1	NOR ARMY LAND WARFARE CENTRE	bskredlund@mil.no
Jorn Georg	MERINGDAL	NOR	OF-4	JWC	joern.meringdal@iwc.nato.int
Robert	BOŽIČ	SVN	OR-8	COMBAT TRAINING CENTER	robibozo@gmail.com
Robert	GLAVAS	SVN	OF-5	COMBAT TRAINING CENTER	rglavas@hotmail.com
Nicholas	BERTEL	SWE	OF2	WEAPON INTELLIGENCE 133 SKV/LG	nicholas.berTEL@mil.se
Fredrik	BRAN	SWE	OF2	WEAPON INTELLIGENCE 133 SKV/LG	fredrik.bran@mil.se
Markus	FREDMAN	SWE	OR6	WEAPON INTELLIGENCE 133 SKV/LG	marcus.fredman@mil.se
Mark	BENN	USA	CIV	JIEDDO / JET	mark.benn1@us.army.mil
Leonard	HAIDL	USA	OF-4	JIEDDO	leonard.haidl@jieddo.mil
Glen	KELLY	USA	CIV	JIEDDO - PMJMT/CJIMRC	calvin.g.kelly.civ@mail.mil
Owen	MURPHY	USA	CIV	JIEDDO / JCOE	owen.murphy@us.army.mil
Ashley	SCHNEIDT	USA	CIV	JIEDDO/J5	ashley.schneidt@jieddo.mil
Robert	VISNOVSKY	USA	CIV	TEDAC/ Intelligence Unit (IU)	ROBERT.VISNOVSKY@IC.FBI.GOV
Thomas	O'BRIEN	USA	CIV	JIEDDO	thomas.obrien@jieddo.mil
Kim Allan	FOG	DNK	OR9	ARMY OPERATIONAL COMMAND / CIED BRANCH	HOK-CIED06@MIL.DK
Pavol	ZIDEK	SVK	OF-2	General staff of Slovak Armed Forces	pavol.zidek@mil.sk
Rupert	TEPLY	AUT	OF-5	Engr School AAF	rupert.teply@bmlvs.gv.at